UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ROKU INC.,
Petitioner,

v.

VIDEOLABS, INC.,
Patent Owner

Case Nos. IPR2024-01023, IPR2024-01024, IPR2024-01025, IPR2024-01026
U.S. Patent Nos. 8,291,236 and 8,667,304

DECLARATION OF DR. SAM MALEK IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSES

TABLE OF CONTENTS

Page

I. INTRODUCTION AND BACKGROUND 3
II. QUALIFICATIONS 4
III. MATERIALS CONSIDERED 10
IV. LEGAL PRINCIPLES 11
V. PERSON OF ORDINARY SKILL IN THE ART ("POSITA") 16
VI. BACKGROUND 17
A. Overview of the '236 and '304 Patents 17
B. Prosecution History of the '236 Patent and '304 Patents 19
VII. SUMMARY OF Russ (EX1005) 20
VIII. DETAILED ANALYSIS OF PETITION GROUNDS 24
A. Dr. Wasilewski fails to show that Russ discloses "a second root of trust," as required by all challenged claims. 24
B. Dr. Wasilewski fails to show that Russ discloses "a second root of trust which is independent of and different than the first root of trust," as required by all challenged claims. 28
A. Dr. Wasilewski's obviousness theories do not cure the deficiencies of Russ. 34
IX. CONCLUSION 35

IPR2024-01024
VideoLabs EX2001

I, Dr. Sam Malek, declare under penalty of perjury as follows:

I. INTRODUCTION AND BACKGROUND

1. I have been retained as an expert witness on behalf of VideoLabs, Inc. ("VideoLabs") to provide information and assistance regarding U.S. Patent Nos. 8,291,236 (the "'236 patent") and 8,667,304 (the "'304 patent"). Specifically, I have been asked to consider the Petitions for Inter Partes Review numbered IPR2024-01023, IPR2024-01024, IPR2024-01025, and IPR2024-01026 (collectively, the "Petitions") regarding the '236 and '304 patents, and specifically the declarations of Dr. Wasilewski that accompanies each Petition as Exhibit 1003.

2. In this declaration I provide my independent analysis of the '236 and '304 patents in light of the materials cited below and discussed herein and my knowledge and experience in this field during the relevant time frame. I have been asked to consider what one of ordinary skill in the art at the time of the invention of the '236 and '304 patents (a "POSITA," see Section V below) would have understood from the specification, including scientific and technical knowledge related to the patents. I have also been asked to consider whether certain references anticipate or would have rendered obvious the inventions described in the claims of the '236 and '304 patents.

3. My findings, as explained below, are based on my study, experience, and background in the fields discussed below, informed by my education and my

extensive experience in the field of content protection and distribution. I have also relied on my review and analysis of the references identified by Dr. Wasilewski, information provided to me, and information that I have independently reviewed. I have personal knowledge of the facts and opinions set forth in this declaration, and, if called upon to do so, I would testify competently thereto.

4. I am being compensated for my independent analysis as an expert with respect to this inter partes review proceeding. My compensation is not contingent in any way on the content of my analysis, the opinions that I offer, or the outcome of this proceeding. I have no financial interest in Petitioner (Roku) or Patent Owner (VideoLabs) and I have no financial interest in the either the ’236 or ’304 patents.

II. QUALIFICATIONS

5. My qualifications for forming the opinions given in this declaration are summarized here and are addressed more fully in my curriculum vitae, which is submitted as EX2002. That exhibit also includes a list of my publications.

6. I have approximately 25 years of experience in the general area of computer and software technology in a variety of roles, including as a software engineer, software architect, and programmer at a variety of companies, as well as a researcher and professor at several universities.

7. I am currently a Full Professor of Software Engineering with tenure in the Informatics Department within the School of Information and Computer

Sciences at the University of California, Irvine. I am also the Director of the Software Engineering and Analysis Laboratory ("SEAL"). My general research interests are in the field of software engineering, and to date my focus has spanned the areas of software analysis and testing, mobile computing, architecture and design, and software dependability and security. The underlying theme of my research has been to devise techniques and tools that aid with the construction, analysis, and maintenance of largescale software systems.

8. I received my Ph.D. and M.S. degrees in Computer Science from the University of Southern California and my B.S. degree in Information and Computer Science from the University of California, Irvine. I have received numerous awards for my research contributions, including the Test of Time Award from the Association for Computing Machinery Special Interest Group on Software Engineering (2020), National Science Foundation CAREER award (2013), GMU Emerging Researcher/Scholar/Creator award (2013), and the GMU Computer Science Department Outstanding Faculty Research Award (2011).

9. I have authored over 130 peer-reviewed research publications. These publications have been highly cited (more than 11,000 times according to scholar.google.com). Many of my publications have dealt with the topics that are related to this proceeding, including distributed software systems, access control, and content protection and distribution. I provide a few examples here.

10. My Ph.D. dissertation resulted in novel algorithms for optimizing the deployment architecture of a distributed software system. The deployment architecture of a distributed software system is the allocation of its software components to its hardware devices. There are many deployments of a software system possible, but some may be superior to others with respect to certain quality of service objectives (e.g., latency, availability, security). One application of my dissertation work was in the context of cloud computing, because in most cloud-based software systems there are many geographically distributed nodes (servers) available for the deployment of software components.

11. In another article titled "GLIDE: A Grid-based Lightweight Infrastructure for Data-intensive Environments," I described the results of my work with colleagues from NASA in the development of a new distributed software system for sharing large amounts of content (e.g., images, videos) generated by NASA. This capability was the first of its kind in the realm of Grid Computing, which is a precursor to Cloud Computing.

12. A significant focus of my work has been on computer security, including electronic forms of access control and management of privileges in software systems. For instance, I led a team of researchers in a project sponsored by the Defense Advanced Research Project Agency (DARPA) to develop a novel approach for protecting Android applications from various forms of access control

attacks. The project resulted in the development of a tool called COVERT. I have published extensively on this work, including a highly cited manuscript that appeared in the IEEE Transactions on Software Engineering in 2015. In another project, I developed DelDroid, which at the time was the first approach for automated determination and enforcement of least privilege architecture in Android. This work was published in the Journal of Systems and Software in 2019.

13. Another thrust of my research has dealt with distribution and accessibility of digital contents. For instance, in a recent article, titled "Automated Accessibility Analysis of Dynamic Content Changes on Mobile Apps," that is slated for publication in the proceedings of the International Conference on Software Engineering, I investigated the impact of dynamically changing contents, such as animations and videos, on blind users.

14. I have received numerous research grants from a variety of organizations, including the National Science Foundation (NSF), Federal Bureau of Investigation (FBI), Air Force Office of Scientific Research, Department of Homeland Security (DHS), National Security Agency (NSA), Defense Advanced Research Projects Agency (DARPA), Office of the Director of National Intelligence, and Army Research Office among others. Software systems and results produced in my research lab have been adopted for use by various organizations in both private (e.g., Boeing, Bosch) and public (e.g., NASA, DHS, FBI) organizations. Many of

the above-mentioned projects and software systems involved analysis and design of client-server software systems deployed on distributive systems. For instance, in a project called "RASS: Resilient Autonomic Software Systems" funded by Air Force Office of Scientific Research, I led a team of researchers to develop a new method of automatically adapting the Air Force's software systems to fluctuations in communication networks, thereby making them resilient to network interruptions.

15. I also have several years of experience as a software engineer, software architect, and programmer at a variety of companies, namely the Boeing Company, PricewaterhouseCoopers Consulting (later acquired by International Business Machines ("IBM") Corporation), FieldCentrix, and Neural Computing Systems Lab. During my tenure in the industry, I gained professional experience in the design, development, and management of largescale software engineering efforts. Among the software systems that I designed and developed were commercial ecommerce and enterprise software systems. Many of the software systems developed in the context of my professional experience were built according to the general client-server architectural style and involved exchange of audio/visual content. For instance, at PricewaterhouseCoopers, I was a member of a software engineering team tasked with developing a web-based solution for exchange of various forms of content, including documents, and audio and video recordings for a large energy company. At Neural Computing Systems Lab I developed solutions for detection of

camouflaged objects (e.g., a military tank) in video and image contents obtained, for instance, through satellites. At Boeing, I worked on a large military modernization program called Future Combat Systems, as part of which I helped with architecting efficient solutions to protect the confidentiality of video/audio content sent from unmanned vehicles (e.g., drones) to base stations.

16. I have taught software engineering and computer science courses on a regular basis at the B.S., M.S., and Ph.D. levels at the universities where I have been employed. I cover concepts related to distributed software, client-server architectural style, authentication, encryption techniques, access control mechanisms, content distribution, and protocols for exchange of electronics credentials (e.g., electronic keys, passwords, and tokens) in many of the courses that I teach at the university.

17. I have been a frequent speaker at scientific conferences, symposia, workshops, and gatherings of software engineering academics and professionals. I have served as chair, committee member, and reviewer for numerous software engineering journals, magazines, and conferences. I have served on the editorial board of the ACM Transactions on Software Engineering and Methodology, IEEE Transactions on Software Engineering, the ACM Transactions on Autonomous and Adaptive Systems, the Springer Journal of Automated Software Engineering, and the Springer Journal of Computing. I am a member of the Association for Computing

Machinery (ACM), ACM Special Interest Group on Software Engineering (SIGSOFT), and the Institute of Electrical and Electronics Engineers (IEEE).

18. I have testified at trial and deposition as an expert witness in numerous cases in the past five years. Several of these cases have involved technologies related to televisions, distribution of audio/video content over networks, and access control. For instance, in 2023, I testified as a software expert in a patent lawsuit between Netflix and GoTV Streaming LLC, focusing on matters related to content display on televisions, in the Central District of California.

III. MATERIALS CONSIDERED

19. In preparing this declaration and forming my opinions, I have considered: the claims, specifications, and prosecution histories of the ’236 and ’304 patents; the Petitions and declarations by Dr. Wasilewski (including all materials cited in each); and all materials cited and discussed in this declaration. In addition, I have considered the relevant legal standards, as they have been explained to me by counsel and as I understand them. I have also considered the knowledge and understanding of a person of ordinary skill at the time of the invention of the ’236 and ’304 patents, of which I am familiar. As part of my analysis for this matter, I have also considered my own knowledge and experience, including my work and experience with content protection and distribution systems.

IV. LEGAL PRINCIPLES

20. In forming my opinions here, I have applied the following understanding of certain legal concepts related to anticipation, obviousness, combinations of references, and knowledge of one of ordinary skill in the art. Counsel for Patent Owner has informed me of legal principles that apply in this proceeding.

21. It is my understanding that assessing the validity / patentability of a U.S. patent claim based on a prior art analysis requires two essential steps. First, one must analyze the terms of the patent claims to understand what meaning one of ordinary skill in the art would give the terms. Second, one may then assess validity by comparing a patent claim to the "prior art." I understand that the teaching of the prior art is viewed through the eyes of a person of ordinary skill in the art at the time the invention was made. My opinion as to what constitutes a relevant person of ordinary skill in the art is set forth below.

22. I have been informed that in order for a patent claim to be invalid as anticipated by a prior art reference under 35 U.S.C. § 102, each and every element of that patent claim must be found disclosed in that reference, explicitly or inherently, to a person of ordinary skill in the art. Inherent disclosure requires that the claimed element be the only possible option given the other disclosures of the reference, and that it would be so recognized by persons of ordinary skill in the art.

I also understand that the missing descriptive material cannot merely be probably or possibly present. If any single element of a claim is not disclosed in the reference, the entire claim is not anticipated. I understand that a prior art reference merely capable of being modified so as to operate in the same manner as the patented device or system does not anticipate. I further understand that obviousness is not inherent anticipation, and that it is insufficient that a missing limitation is so similar to a limitation actually disclosed in the reference that one of ordinary skill in the art would see the substitution as obvious. I also understand that, if it is necessary to reach beyond the boundaries of a single reference to provide missing disclosure of the claimed invention, the proper ground for asserting invalidity is not anticipation, but obviousness.

23. I understand that a claim is invalid as obvious under 35 U.S.C. § 103 if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art.

24. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and the claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

25. I have been informed that the following factors are used to determine whether or not the claimed subject matter would have been obvious: (i) the scope and content of the prior art; (ii) the differences between the prior art and the claimed invention; (iii) the level of ordinary skill in the field of the invention; and (iv) any relevant objective considerations of non-obviousness, such as commercial success, long-felt but unresolved needs, failure of others, etc.

26. I also understand that in considering the scope and content of the prior art, references must be reasonably related (i.e., analogous) to the claimed invention of that patent. I understand that the test for determining whether a prior art reference constitutes analogous art to the claimed invention is (1) whether the reference is from the same field of endeavor, regardless of the problem addressed and, (2) if the reference is not within the field of the inventor's endeavor, whether the reference is still reasonably pertinent to the particular problem the inventor is trying to solve.

27. I understand that a party asserting obviousness based on a combination of prior art references must demonstrate that one of ordinary skill in the art would have been motivated to combine the teachings of those references to achieve the claimed invention and that the skilled artisan would have had a reasonable expectation of success in doing so. It is my understanding that it is not enough to show that one skilled in the art could combine elements of multiple references, but instead there must be some reason that would have prompted a person of ordinary

skill in the art to combine the elements in the way the claimed invention does. I understand that there must be some reasoned explanation as to why one of ordinary skill in the art would combine the references. The reason cannot come from hindsight.

28. I understand that in considering whether a claimed invention is obvious, one may but is not required to find obviousness if at the time of the claimed invention there was a reason that would have prompted a person having ordinary skill in the field of the invention to combine the known elements in a way the claimed invention does, taking into account such factors as: (1) whether the claimed invention was merely the predictable result of using prior art elements according to their known function(s); (2) whether the claimed invention provides an obvious solution to a known problem in the relevant field; (3) whether the prior art teaches or suggests the desirability of combining elements claimed in the invention; (4) whether the prior art teaches away from combining elements in the claimed invention; (5) whether it would have been obvious to try the combinations of elements, such as when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions; and (6) whether the change resulted more from design incentives or other market forces. To find it rendered the invention obvious, the prior art must provide a reasonable expectation of success. Obvious to try is not sufficient in unpredictable technologies.

29. I understand that each claim must be evaluated separately for obviousness, and that it is improper to use hindsight. I understand that the disclosures in a patent or a prior art reference are viewed from the perspective of a person of ordinary skill in the art at the time of the invention. The obviousness analysis by a person of ordinary skill in the art must consider only what was known at the time of the invention.

30. It is my further understanding that obviousness cannot be based on a hindsight combination of components selected from one or more prior art references. I also understand that an invention would not have been obvious simply because all of the elements of the invention may have been known separately in the prior art.

31. I understand that a combination of disclosures or references would not have been obvious if the alleged modification(s) to be made to the reference(s) would have been inconsistent with the reference's stated goals or would have rendered the combination inoperable for its intended purpose. I further understand that for something to have been obvious, the party asserting obviousness must explain why a POSITA would have selected components or features for combination in the manner claimed.

32. I have been informed that a prior art reference must be considered in its entirety, i.e. as a whole, including portions that would lead away from the claimed invention.

33. I understand that with respect to claim construction, the proper construction is considered in the context of, and must be consistent with, the specification and that the claim language should be read in light of the specification and file history as it would be interpreted by one of ordinary skill in the art.

V. PERSON OF ORDINARY SKILL IN THE ART ("POSITA")

34. Counsel for Patent Owner has informed me that a person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. In my opinion, the relevant field of art for the '236 and '304 patents is that of content protection and distribution.

35. For the purpose of this Declaration, and based on my opinions herein, the time of invention for the '236 and '304 patents is the late 1990s to early 2000s. Any invention date in this general timeframe would not alter my opinion regarding a person of ordinary skill in the art.

36. I have been informed by counsel for Patent Owner that the person of ordinary skill is generally familiar with the type of problems encountered in the field and the prior art solutions to those problems and possesses an ordinary level of creativity.

37. I understand that Petitioner's expert, Dr. Wasilewski, opined that a person of ordinary skill in the art "would have had a bachelor's degree in computer science, computer or electrical engineering, or a related field, and approximately two

or more years of experience in computer and networking technology. Additional education could substitute for less professional experience, and vice versa." IPR2024-01023, EX1003, 01023 Wasilewski Decl., ¶ 48.[1]

38. For purposes of this declaration, I apply Dr. Wasilewski's definition. However, I note that the opinions I set forth below are applicable under any reasonable definition of a POSITA. I also note that I qualify as a POSITA under Dr. Wasilewski's proposed definition.

VI. BACKGROUND

A. Overview of the '236 and '304 Patents

39. U.S. Patent No. 8,291,236 (the "'236 patent"), is titled "Methods and Apparatuses for Secondary Conditional Access Server," issued on October 16, 2012. '236 Patent[2], Face Page. U.S. Patent No. 8,667,304 issued on March 4, 2014, and,

[1] My declaration discusses four declarations from Dr. Wasilewski in cases IPR2024-01023-01026 where, for purposes of this Declaration, Dr. Wasilewski expresses substantively the same opinions. Unless noted otherwise, my analysis herein applies to each of the four Petitions and Dr. Wasilewski's opinions in each of the separate petitions.

[2] The '236 Patent is EX1001 in IPR2024-01023-01025. The '304 patent is EX1001 in IPR2024-01026.

as it is a continuation of the ’236 patent, shares a common specification. As such, I will discuss the two patents together, and my discussion applies to each patent.

40. Generally, the ’236 and ’304 patents describe bridging two separate security domains. ’236 Pat., Abstract. A first security domain could be, for example, “a broadcast CA system,” such as a cable television broadcast system. *See id.*, 2:61-67 and Fig. 3. A second security domain could be “a digital rights management system,” such as used for streaming content over the Internet; it could also be a separate CA system from a cable broadcast system, such as satellite television. *Id.* Before the invention of the ’236 and ’304 patents, each device displaying content from one of these systems had to be subscribed to and authenticated by the system. *See, e.g.*, ’236 Pat., 9:60-64. ’236 File History[3], 381. However, different devices could not be authenticated in differing security domains. *See, e.g.*, EX1001, 9:60-64 (describing needing two separate set-top boxes for two different domains). The patents describe a “secondary access server” that could independently verify devices. *See, e.g.*, ’236 Pat., 8:3-38, claim 130. The secondary access server could provide content from various security domains to the verified device, without the device having to be verified within each security domain. *Id.*; *see also* ’236 File History, 381.

[3] EX1002 in IPR2024-01023-01025 and EX1015 in IPR2024-01026.

B. Prosecution History of the ’236 Patent and ’304 Patents

41. The prosecution history describes that “[i]n the prior art approaches, a client of a secondary CA server would need to subscribe to the primary CA server in order to receive services from the primary CA server.” ’236 File History, 478. The inventions allow “a user to receive secured content from a primary system without directly subscribing to the primary system services.” *Id.*, 479. After independently authorizing its clients, the secondary CA may receive data from the first security domain and provide it to its clients, without the clients needing to subscribe to the first security domain or be authenticated within the first security domain, allowing for “two security systems having two independent authentication processes.” *Id.* During prosecution, the inventors also disclosed that the two authentication processes “use two different roots of trust that are independent.” *Id.*, 477.

42. The inventors distinguished references in prosecution that disclosed only “a single DRM system.” *Id.* The Simelius reference discussed in prosecution, for example, disclosed a parent client and a child client with the single DRM system. *Id.* In that reference, “[t]he parent client must verify that the child client public key is chaining to the root of trust of the content server.” *Id.* As disclosed in the prosecution history, this disclosure of Simelius did not disclose two independent authentication processes using two independent roots of trust, but taught that a parent

client could "act as authentication proxy" for child clients in the same DRM system. *Id.*, 478.

43. In the prosecution of the continuation '304 patent, the Examiner issued a double patenting rejection, which was overcame via terminal disclaimer. IPR2024-01026, EX1002, 94, 136.

VII. SUMMARY OF RUSS (EX1005)

44. U.S. Patent No. 6,748,080 (EX1005, "Russ") is titled "Apparatus for Entitling Remote Client Devices." Russ is directed to a single "subscriber network." Russ describes a "digital broadband delivery system" (e.g., Fig. 1) that provides audiovisual content, such as television content, to users' devices. EX1005, 1:14-16; *see also id.*, 3:11-12 (embodiments described "in a subscriber television network."). In Russ, access to this content is provided and controlled by a "headend 102," as illustrated in Fig. 1. Russ's network includes a "Headend 102" and a DSCT 110 connected to subscriber devices (e.g., TV and laptop as illustrated) via wired and wireless connections. *Id.*, Fig. 1. Russ's headend 102 provides content to subscriber devices within the subscriber network. *Id.*, 1:15-24. The headend manages encryption of communications between devices in the network and manages which devices in the network are authenticated for receiving content. *Id.*, 25:17-22.

45. Like conventional television subscriber systems, Russ's system includes, at "a subscriber location, a digital subscriber communications terminal

(DSCT)," such as a set-top box. *Id.*, 1:36-44. As a POSITA would have understood, a device such as a DSCT was typically connected to a television or other device via wired connection such that they receive content "from the subscriber network." *Id.* Russ asserted that, as portable devices were coming available, it would be "desirable to couple subscriber device to the DSCT using wireless communication." *Id.*, 1:46-64. This wireless communication would allow "the subscriber to easily move his or her portable computing device … while remaining connected to the subscriber network through the subscriber's DSCT." *Id.*

46. Russ discloses that connecting wirelessly to the DSCT "introduce[s] security and control concerns for the operators of the subscriber network system." According to Russ, "communication signals over wireless links are more readily intercepted than signals over wired links, wireless communication links are inherently less secure." *Id.*, 2:63-66. Russ therefore proposed encrypting information communicated from the DSCT to a wireless subscriber device. *See e.g.*, *id.*, 25:19-25. Russ describes that a "headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122." *Id.*, 25:17-22. Russ also taught that its headend would dictate and control encryption schemes for communication of content between the DSCT 110 and client-receiver 122 through use of tables. Russ discloses that "[s]ystem tables are prepared by the control system 232 [of headend 102] and transmitted to the DSCT 110." EX1005,

14:50-55; *id.*, Fig.2 (control system 232 is part of headend 102). DSCT stores the tables in its memory. *Id.*, 14:50-55. Once the DSCT receives a message from a client-receiver 122, the client-receiver is identified by the headend, either using the tables provided by the headend or by the forwarding of the message to the headend. The headend, via its own processor or the tables "identif[ies] a client-receiver" and, based on the device type of the client-receiver, determines what encryption to apply. *Id.*, 16:43-50, 16:55-63; *see also id.*, 17:24-29 (the DSCT uses the tables from the headend to identify an encryption scheme). Although Russ describes multiple ways to do so, a POSITA would have understood that, in Russ's system, the headend controls encryption. The headend also controls whether encryption occurs at all: "[t]he system controller 232 can also send an EMM to the DSCT 110 instructing the processor 312 to no longer determine the encryption scheme for the client-receiver 122." *Id.*, 25:17-19.

47. In addition to security concerns via wireless transmission, Russ was further concerned with the operator of the subscriber network, who "wants the capability to control the type of devices that receive information from the DSCT or the type of content that the device receives." *Id.*, 2:66-3:2; *see also id.*, 2:55-60 ("The operator of a subscriber network system desires the ability to entitle (or disentitle) subscriber devices, i.e., to enable (or prevent) the subscriber devices from accessing communication transmitted over a local area network, which may include wired

communication links, wireless communication links, or a combination thereof."). As Russ wants the operator of the subscriber network to perform this control, it discloses the headend 102 performing the control. The control system of the headend "allows the DBDS [digital broadband delivery system] system operator to control and monitor the functions and performance of the DBDS" including "conditional access for the content distributed to subscribers." *Id.*, 10:25-34. "The DSCT 110 receives entitlements for the service instances from the Entitlement Generator 236 of the control system 232." Id., 15:43-45. "The system controller 232 can also block services or service instances. In that case, the system controller 232 sends messages and/or tables to the DSCT 110 that instruct the DSCT 110 which types of client-receiver devices can receive which type of service or service instance." Id., 24:52-53. Moreover, "the system controller 232 can send an EMM 800 to the AEMM 720 that suspends the entitlements of the client-receiver 122 to service instances. The system controller 232 can send an entitlement suspension EMM that suspends the entitlement of a specific client-receiver 122 coupled to the DSCT 110 or all client-receivers coupled to the DSCT 110. The system controller 232 may send an entitlement suspension EMM based upon the hardware type of the client-receiver 122." *Id*., 24:67-25:7.

48. The headend of the subscriber network controls both an initial connection, conditional access authority, and encryption schemes for the client-

receivers. *See id.*, 2:55-3:10. While a DSCT in a subscriber's home may pass content to a client-receiver of the subscriber, the network operator, via the headend, controls what content can be provided to which device and how that content is delivered. The DSCT "acts as a proxy" under the control of the headend. *See id.*, 19:24-26.

VIII. DETAILED ANALYSIS OF PETITION GROUNDS

49. As I describe in detail below, it is my opinion that Dr. Wasilewski and the Petitions fail to demonstrate any reasonable likelihood of success that any challenged claim of the '236 or '304 patents is invalid. I understand that the challenged independent claims are claims 32, 48, 66, 82, 100, 116, 130, and 140 of the '236 patent and claims 5 and 6 of the '304 patent. Each challenged independent requires "a second root of trust" "which is independent of and different than the first root of trust." In my opinion, Dr. Wasilewski fails to demonstrate that Russ discloses or renders obvious this limitation for two separate reasons. First, it is my opinion that Dr. Wasilewski fails to identify any "second root of trust" in Russ. Moreover, even if there was a second root of trust, Dr. Wasilewski fails to show that it "is independent of and different than the first root of trust."

A. Dr. Wasilewski fails to show that Russ discloses "a second root of trust," as required by all challenged claims.

50. All challenged claims require a "second root of trust." In my opinion, Dr. Wasilewski fails to demonstrate that Russ discloses a second root of trust

because a POSITA would not understand the functionality that Dr. Wasilewski is relying on to be disclosed by Russ. For the second root of trust, Dr. Wasilewski points to Russ's disclosure of DTCP encryption. Particularly, he relies on an Authentication and Key Exchange (AKE), "which is based on a certificate used by a trusted authority, such as DTLA." 01023 Wasilewski Dec., ¶¶ 98-102.[4] However, Russ does not mention an AKE or DTLA certificate and, in my opinion, a POSITA would not understand Russ to disclose the purported "second root of trust" that Dr. Wasilewski identifies.

51. For context, I will provide a brief background of authentication and confidentiality. Generally, communications between devices can involve separate concepts of authentication and confidentiality. Authentication is the principle of verifying that a device is *who* or *what* it claims to be. Authentication is typically achieved through exchange of credentials, like passwords, biometrics, security tokens, or cryptographic keys. Confidentiality, on the other hand, is the principle of keeping information private. It is primarily achieved through encryption of information. Even if an unauthorized, non-authenticated entity gains access to certain encrypted information, the information remains private because the

[4] *See also* 01024 Wasilewski Dec., ¶¶ 95-99; 01025 Wasilewski Dec., ¶¶ 127-131; 01026 Wasilewski Dec., ¶¶ 90-94.

unauthorized entity cannot decrypt it to read its content. I note that Petitioner's Exhibit 1041 explains this concept. As shown there, authentication is distinct from and occurs prior to transmission of encoded content. EX1012, ¶ 41. A device may be authenticated without providing any encrypted communications. Likewise, encrypted information may be transmitted to a device without authentication.

52. For his theory, Dr. Wasilewski relies only on one paragraph in Russ, which is related to confidentiality and not authentication. *See* EX1005, 16:65-67. Russ discloses that content transmitted to a client-receiver 122 may be "transmitted so as to protect the privacy of the communication." EX1005, 16:65-67. To do so, Russ says that any "encryption scheme," could suffice and provides an example of several such schemes, including Digital Transmission Content Protection (DTCP). *Id.*, 17:7-14. As explained above, after a device is authenticated, content can then be provided to it using an encryption scheme, such as DTCP or other "encryption schemes[]" "known to those skilled in that art." EX1005, 17:7-14. However, as a POSITA would understand, merely encrypting information does not disclose how (or if) any device was authenticated such that it could decrypt information.

53. While Russ discloses utilizing DTCP's encryption scheme, a POSITA would not understand Russ to disclose using DTCP for authentication. Dr. Wasilewski opines Russ discloses authentication using an AKE key exchange between DSCT 110 and client-receiver 122, using DTLA licensed certificates.

01023 Wasilewski Dec., ¶ 101.[5] Dr. Wasilewski further opines that DTLA certificates are "issued by a trusted authority" which establishes a "root of trust." *Id.*

54. A key exchange, such as AKE, would provide the client-receiver 122 information, a "key," that could be used to decrypt communication. However, Russ does not disclose any AKE key exchange or any DTLA licensed certificates. Instead, Russ explicitly discloses exchanging trusted keys without the need for DTLA certificates. Russ discloses that a serial number and keys that are assigned to a client-receiver are included in a client-receiver 122 during the manufacturing process. EX1005, 26:29-48. The manufacturer provides the serial number and a key to the operator of Russ's DBDS (the subscriber network), which is operated by the headend 102. *Id.* When the device comes online, the DSCT 110 forwards the serial number of the device to the headend 102's CAA (content access authority). *Id.* EX1005, 26:29-48. The headend then confirms whether it has received the serial number and keys from the manufacturer. *Id.* If so, the CAA of the headend "sends the client-receiver 122 via, the DSCT, an EMM that includes the public key of the DSCT 110," and "the client-receiver 122 accepts the public key of the DSCT 110 as a trusted key." *Id.* A POSITA would therefore understand that Russ describes a process of

[5] *See also* 01024 Wasilewski Dec., ¶ 98; 01025 Wasilewski Dec., ¶ 130; 01026 Wasilewski Dec., ¶ 96.

authenticating devices by exchanging keys that does not involve AKE key exchange or certificates of the DTLA, the alleged "trusted authority." In my opinion, a POSITA would thus understand that Dr. Wasilewski fails to demonstrate that Russ discloses a "second root of trust."

B. Dr. Wasilewski fails to show that Russ discloses "a second root of trust which is independent of and different than the first root of trust," as required by all challenged claims.

55. In my opinion, Dr. Wasilewski does not demonstrate that a POSITA would have understood Russ to disclose a "second root of trust which is independent of and different than the first root of trust," as recited in all challenged independent claims.

56. As an initial matter, Dr. Wasilewski does not sufficiently explain why it is his opinion that that the two alleged roots of trust he identifies are independent. Instead, he appears to opine that the second root of trust is independent from the first root of trust because it is different. 01023 Wasilewski Dec., ¶ 101.[6] Indeed, as highlighted in the prosecution history of the '236 patent, the claimed second root of trust must not only be "different" from the claimed first root of trust, it must also meet the second requirement of being independent. '236 File History, 479. As Dr.

[6] *See also* 01024 Wasilewski Dec., ¶ 98; 01025 Wasilewski Dec., ¶ 130; 01026 Wasilewski Dec., ¶ 96.

Wasilewski provides no reason why the alleged second root of trust is independent from the alleged first root of trust other than that the two are "different," it is my opinion that Dr. Wasilewski fails to establish or provide any reason or analysis for the "independent" requirement. As Dr. Wasilewski has not demonstrated that Russ discloses this claim element, he cannot show that Russ anticipates the challenged claims.

57. It is my opinion that Russ does not disclose a second root of trust that is independent from a first root of trust, as any root of trust for Russ's client-receiver 122 is dependent on a root of trust for Russ's DSCT 110. Dr. Wasilewski opined that the "first root of trust" is "a unique serial numbers and keys" included in DSCT 100. 01023 Wasilewski Dec., ¶ 95.[7] He then opines that the headend 102, the "operator of the DBDS 100," uses this unique serial number and keys to authenticate and establish communications with the DSCT. *Id.* Dr. Wasilewski similarly opines that the alleged "second root of trust" is in Russ's exchanging information from client-receive 112 (through an AKE process), allowing communication between the DSCT

[7] *See also* 01024 Wasilewski Dec., ¶ 92; 01025 Wasilewski Dec., ¶ 124; 01026 Wasilewski Dec., ¶ 83.

110 and client-receiver 112 to subsequently take place. 01023 Wasilewski Dec., ¶ 101.[8]

58. Under Dr. Wasilewski's alleged roots of trust—or any two roots of trust—Russ states that it is a purpose of his system to have the two purported roots ***not*** be independent. Russ explains that the operator of a subscriber network system (headend 102) controls communication between the DSCT and subscriber devices, including "control the type of devices that receive information from the DSCT or the type of content that the device receives." EX1005, 2:5-3:10. Toward this end, the operator "establish[es] secure communication with the client-devices and control[s] the content that is provided to the client-devices." *Id.* The operator controls the system using the headend 102 and its system controller 232. *Id.* 10:25-29 ("control system 232 … allows the DBDS system operator to control and monitor the functions and performance of the DBDS 100."). As such, Russ makes clear throughout that the headend 102 controls any authentication of client-receiver, controls what content it can receive, controls encryption of content, and can, at any time, remove a client-receiver as an authorized device. *See, e.g.*, EX1005, 25:17-25, 16:43-50, 16:55-63, 17:24-29, 2:55-3:2, 10:25-34, 15:43-45, 24:52-53, 24:67-25:7.

[8] *See also* 01024 Wasilewski Dec., ¶ 99; 01025 Wasilewski Dec., ¶ 130; 01026 Wasilewski Dec., ¶ 93.

59. A POSITA would understand that the headend 102 controls access to client-receivers via the DSCT. Russ's headend 102 establishes communications with the DSCT 110 and then the headend 102 controls the client-receivers by communicating with the DSCT 110. For example, as Dr. Wasilewski explains, the headend 102 controls entitlement instances. 01023 Wasilewski Dec., ¶ 57.[9] In Dr. Wasilewski's opinion, his alleged second root of trust is initiated through "DTCP protocols" which are initiated after it is determined to use the DTCP encryption scheme for communications between DSCT 110 and client-receiver 122. 01023 Wasilewski Dec., ¶ 98.[10] However, as Dr. Wasilewski recognizes, the headend 102 controls this dynamic encryption. 01023 Wasilewski Dec., ¶ 91[11]; *see also* EX1005, 25:17-22 ("headend 102 determines the encryption scheme used to communicate information between the DSCT 110 and the client-receiver 122"); *id.*, 14:50-55 (encryption scheme determined by tables sent from the headend 102 to DSCT 110). As such, a POSITA would understand that for the DSCT 110 to "determine" the

[9] *See also* 01024 Wasilewski Dec., ¶ 61; 01025 Wasilewski Dec., ¶ 83; 01026 Wasilewski Dec., ¶ 63.

[10] *See also* 01024 Wasilewski Dec., ¶ 95; 01025 Wasilewski Dec., ¶ 127; 01026 Wasilewski Dec., ¶ 91.

[11] 01024 Wasilewski Dec., ¶ 83; 01025 Wasilewski Dec., ¶ 120; 01026 Wasilewski Dec., ¶ 103.

encryption scheme, it requires instructions from the headend 102. Those instructions are communicated to the DSCT 110 only after establishing a first root of trust between the headend 102 and DSCT 110. *See, e.g.*, EX1005, 7:56-8:3. Thus, without the first root of trust, the alleged second root of trust cannot be established. A POSITA would thus understand that any root of trust between the DSCT 110 is intrinsically tied to and predicated on a root of trust between the headend 102 and DSCT 110. The purported second root of trust therefore, while perhaps different, is not independent from the first root of trust, as required by the challenged claims.

60. In my opinion, Dr. Wasilewski's identification of the purported second root of trust (which is not disclosed by Russ) only further shows that Russ fails to disclose a second root of trust that is independent of a first root of trust. For the authentication of the DSCT 110 using the first root, Dr. Wasilewski opines that Russ's "headend 102 authenticates DSCT 110." 01023 Wasilewski Dec., ¶ 94.[12] He opines that the DSCT is manufactured to include a unique serial number and keys, which are provided to headend 102. *Id.* If the headend recognizes the serial numbers,

[12] *See also* 01024 Wasilewski Dec., ¶ 91; 01025 Wasilewski Dec., ¶ 123; 01026 Wasilewski Dec., ¶ 82.

the headend provides DSCT 110 "with a trusted public key." 01023 Wasilewski Dec., ¶ 94.[13]

61. Russ's disclosure for the client-receiver is substantially the same. As Russ discloses, the client-receiver includes a serial number, which is also stored in a database of the DBDS. EX1005, 26:29-48. When the client-receiver is brought online, its serial number is provided to headend 102, which provides a "trusted key" in response—just as with the DSCT 110. *Id.* Tellingly, Dr. Wasilewski ignores this disclosure for the "second root of trust" requirement, because, in my opinion, it highlights why a POSITA would understand that alleged second root of trust is not independent of the alleged first root of trust, as I explained above. That is Russ's operator—the headend 102—controls and performs any authenticating of devices in the DBDS. As the alleged authentication using the second root of trust can only be performed ***after*** the DSCT is authenticated (using the alleged first root of trust), the alleged second root of trust cannot be established without the alleged first root of trust. A POSITA would understand that the alleged second root of trust relies on the alleged first root of trust and the alleged second root of trust is thus not independent.

[13] *See also* 01024 Wasilewski Dec., ¶ 91; 01025 Wasilewski Dec., ¶ 123; 01026 Wasilewski Dec., ¶ 82.

62. Regardless of what the alleged second root of trust for authenticating the client-receiver is in Russ, it cannot be independent of the first root of trust because the client-receiver is authenticated by the headend 102 via DSCT 110, and that cannot be performed without the headend 102 communicating with the DSCT 110, which requires the first root of trust. A POSITA would understand that any second root of trust in Russ cannot be independent of the alleged first root of trust.

A. Dr. Wasilewski's obviousness theories do not cure the deficiencies of Russ.

63. In my opinion, Dr. Wasilewski's obviousness theories do not cure the failures of Russ that I describe above. Under ground 2, Dr. Wasilewski only opines that it would have been obvious to combine separate embodiments of Russ.

64. Dr. Wasilewski makes no effort to cure Russ's deficiencies discussed with respect to ground 1. Instead, he states that it would have been obvious to combine alternative embodiments of Russ, without stating which embodiments he proposes to combine or providing any nonconclusory reason why any nonidentified embodiment would be compatible. 01023 Wasilewski Dec., ¶¶ 186-87.[14] While I disagree, combining disclosures of Russ would not change my opinion that Russ fails to disclose the limitations of the challenged claims that I discuss above. In fact,

[14] *See also* 01024 Wasilewski Dec., ¶¶ 165-66; 01025 Wasilewski Dec., ¶¶ 179-80; 01026 Wasilewski Dec., ¶¶ 122-23.

Dr. Wasilewski's opinions here highlight that Russ is describing a single subscriber network. Russ describes, the headend 102 can be in direct or indirect communication wit subscriber locations as "a matter of implementation." EX1005, 5:57-62. A POSITA would understand this to mean that regardless of the connection type between the headend and the subscriber, whether direct or indirect, it is the headend 102 that controls every aspect of the system, including any authentication of client-receivers.

65. While grounds 3 and 4 include additional references for dependent claims, the references do not cure Russ's deficiencies with respect to the independent claims, and Dr. Wasilewski does not opine otherwise. It is thus my opinion that Dr. Wasilewski fails to demonstrate that any challenged claim is invalid

IX. CONCLUSION

66. This declaration reflects my opinions as currently held. However, my analysis may continue such that I may consider additional information that may result in additional observations.

67. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 18th day of September, 2024, at Vienna, Austria.

Dr. Sam Malek